

REMARKS

New claim 19 has been added and recites no new matter. Support for new claim 19, may be located at page 3, lines 28-31. Claims 12-19 are pending in the application.

On page 2 of the Office Action dated August 8, 2005, claims 12-18 were rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,668,322, issued to Wood *et al.* (hereinafter Wood).

Applicant respectfully submits that claims 12-18 are patentable over Wood, as Wood does not teach each and every element of the claims. In particular, Wood fails to teach, "periodically validating access privileges based on contractual relationship information; and deleting login data or creating login data according to said validating," as recited in independent claim 12.

Wood is directed to a security architecture in which authentication schemes based on passwords, certificates, biometric techniques, smart cards, etcetera, are associated with trust levels. According to Wood, a login service can obtain login credentials for an entity commensurate with a trust level requirement of an information resource to be accessed. When the login credentials have been obtained for an entity and have been authenticated to a particular trust level, session credentials are issued and access is granted to resources for which the trust level is sufficient. According to Wood, by using the session credentials, access is granted without the need for further authentication. See Wood, column 2, lines 38-55.

The present invention provides enhanced and extended computer account authentication and authorization. In at least one embodiment of the present invention, a user's valid contractual relationship with an information system provider may be determined and verified after validating a user's login information such as user identification data and a password. In at least one embodiment of the invention, the contractual relationship can be validated by validating a user identifier with information relating to a contract between the user and the information system provider, such as, content of an insurance contract and/or a contract holder or identifier, for example.

Periodic validation of user eligibility and/or user access privileges may also be performed according to at least one embodiment of the present invention. For example, at a random point in time, the information system of the present invention may perform processing to validate user information by matching user login data to user contractual data referenced when determining user eligibility. User login data may be generated or removed according to the validation. For example, if the user login data does not exist but a valid contractual relationship does exist, the login data may be generated for the user. See Specification of the Present Invention, Page 13, lines 15-30.

The section of Wood cited by the Examiner, that is, column 5, lines 46-57, describes a situation in which an authorization component attempts to obtain authorization for access to an application or resource. If the requesting entity has not been authenticated to a particular trust level required for access to the application or resource, control is redirected to a login component to obtain login credentials and to authenticate to a particular trust level.

Applicant respectfully submits that merely authenticating to a particular trust level is not equivalent to or tantamount to periodically validating access privileges based on contractual relationship information. In contrast to the present invention, in Wood, the authentication occurs based on a current trust level, which is not contractual relationship information.

The second section of Wood cited by the Examiner, that is, column 6, lines 57-67, describes a situation in which login credentials are obtained from a login component and authenticated to a particular trust level.

In contrast to the present invention, in Wood, the login credentials are simply obtained, that is, selected by the login component 120. See Wood, column 5, lines 37-40. No information is provided, in Wood, regarding deleting or creating login data according to periodic validation, as identified in the present invention.

Moreover, in Wood, the authentication occurs in response to a browser user requesting access to a particular enterprise application or information resource. In contrast to the present invention, Wood does not perform periodic validation of access privileges, as identified by the language of claim 12.

In light of the foregoing, Applicant submits that independent claim 12 is patentable over Wood. As claims 13-18 depend from independent claim 12, claims 13-18 are patentable over Wood for at least the reasons offered above with respect to claim 12.

Applicant respectfully submits that claim 19 is patentable over Wood, as Wood does not teach, "periodically validating access privileges based on contractual relationship information; and creating login data independent of an attempt to access information in the system," as recited in claim 19.

There being no further outstanding objections or rejections, it is submitted that the application is in condition for allowance. An early action to that effect is courteously solicited.

Finally, if there are any formal matters remaining after this response, the Examiner is requested to telephone the undersigned to attend to these matters.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

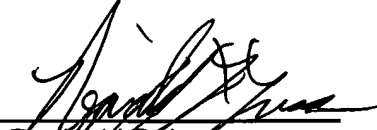
Respectfully submitted,

STAAS & HALSEY LLP

Date:

11/8/05

By:


Reginald D. Lucas
Registration No. 46,883

1201 New York Avenue, NW, Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501